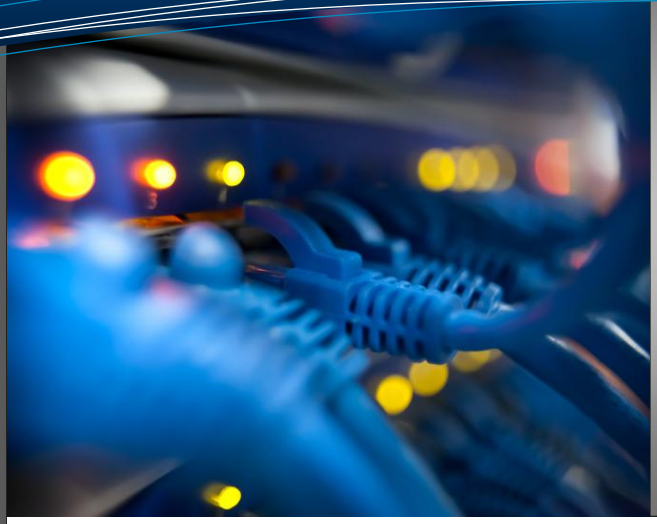
April 2011

MONTHLY Cyber Security Newsletter

Security Tips



Mississippi Department of Information Technology Services

Division of Information Security

What's new this month?

In this issue we will discuss the Epsilon Data Breach and how to avoid being a victim of phishing attacks. Wondering how to secure your home computer and network? Tips included in this month's edition!

Phising Alert – Epsilon Data Breach

On March 30th, Epsilon, a major e-mail marketing services provider experienced a security breach that compromised the customer data of some of the businesses that utilize Epsilon for their e-mail marketing needs. The breach affects over 90 high profile companies including but not limited to drugstore chain Walgreens, electronics chain Best Buy, communications provider Verizon, a number of financial services companies including Capital One, Citibank, JP Morgan Chase, Barclaycard, hotel chain Marriott, bookseller AbeBooks, sports apparel dealer Lacoste and retail supermarket chain Kroger. You can view the link at the end for an up to date list of companies affected.

Epsilon reports that while customer names and email addresses have been exposed, no sensitive personal data was compromised. In the days and months ahead, it is anticipated that spammers and cyber criminals will attempt to exploit the trusted relationships customers may have with companies that use Epsilon for their email marketing needs. Affected companies are urging users to be wary of incoming emails that ask for account updates, as they may be phishing scams. There are already websites that have appeared purporting to represent Epsilon that claim to allow people to find out if they have been affected. These are fake sites and are intended to trick individuals into downloading malicious software.

If you conduct business with any of the impacted firms and have provided them with your email address, you should be on the lookout for communication from these businesses providing details and information about this breach of their data. Please note that any correspondence with affected companies should not ask to the customer to confirm or provide any information.

What Can I Do To Be Safe?

This exposure of emails and customer names may lead to a wave of phishing attacks. Phishing is a vehicle to obtain your personal data, such as credit card numbers, passwords, account data, or other information. The scam attempts to entice email recipients into clicking on a link that takes them to a bogus website. This website may then prompt the recipient to provide personal information such as social security number, bank account number or credit card number, and/or it may download malicious software onto the recipient's computer.

Both the link and website may appear authentic, however they are not legitimate. Legitimate businesses should never ask for personal or financial information via an email that is sent to you.

While targeted phishing attacks are likely to increase as a result of this breach, it is important that users are always vigilant for phishing attacks and understand how to recognize a phishing attempt and what users can do to protect yourself and minimize the likelihood of getting phished. The tips below will help you stay safe.

How Can I Avoid Becoming A Victim?

- Be cautious about all communications you receive including those purported to be from "trusted entities", and be careful when clicking links contained within those messages.
- Do not respond to any unsolicited (spam) incoming e-mails.
- Do not open any attachments contained in suspicious emails.
- Do not respond to an email requesting personal information or that ask you to "verify your information" or to "confirm your user-id and password."
- Beware emails that reference any consequences should you not 'verify your information'.
- Do not enter personal information in a pop-up screen. Providing such information may compromise your identity and increase the odds of identity theft.
- If it appears to be a phishing communication, do not respond. Delete it. You can also forward it to the Federal Trade Commission at spam@uce.gov

Resources For More Information:

- List of Companies Affected by Epsilon Breach:
  - www.bankinfosecurity.com/articles.php?art_id=3505
- MS-ISAC Newsletter on Phishing:
  - www.msisac.org/awareness/news/2008-10.cfm
- FTC's Identity Theft Website:
  - www.ftc.gov/bcp/edu/microsites/idtheft
- NCCIC Advisory on Targeted Phishing Attacks:
  - www.msisac.org/documents/NCCICPhishingAdvisory.pdf
- AntiPhishing Work Group:
  - www.antiphishing.org
- OnGuard Online:
  - www.onguardonline.gov/phishing.html
- US Cert:
  - www.us-cert.gov/cas/tips/ST04-014.html

For more monthly cyber security newsletter tips, visit: www.msisac.org/awareness/news/

this newsletter is brought to you by…

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™
A DIVISION OF CENTER FOR INTERNET SECURITY

www.msisac.org

ITS

www.its.ms.gov/services_security.shtml

Protecting Home Networks/Computers

According to F-Secure, an antivirus software company, 80% of home computers are infected with spyware or adware programs and about 67% of home computers lack current antivirus software. With the rapid growth of new intrusion tactics and viruses, home users need to be more educated than ever before on security measures to take in order to protect their home computers and networks. Listed below are some actions that can be taken in order to make your home network environment more secure and protected against cybercriminals:

1. **Install a firewall** – A firewall is a software program or a hardware device that limits connections to your computer or network. Your firewall should be configured in the most-specific way possible, so that unnecessary ports are not accessible from the Internet. Some operating systems have software firewalls installed, but many of them may default to the "off" mode, so make sure that your firewall is turned on. No firewall will block all attacks so it is not enough to install a firewall and then ignore all other security measures.

2. **Secure your wireless connection** –Change your SSID from the default and don't broadcast it. Change the default password of the admin interface of your wireless router. Enable, at minimum, WPA encryption with a strong password. The encryption will both restrict access to your network and protect your data during transmission.

3. **Install and maintain anti-virus software –** Anti-virus software helps to protect your computer from viruses. Viruses today can steal your personal data, utilize your computer's resources to send spam, slow down and crash your computer, permit an unauthorized user access to your internet connection (for things such as illegal downloads), and many other malicious things. In order to protect against the latest viruses, you must keep your software updated. Use automatic updates to help keep your software current, as it's only as good as its last update.

4. **Install and maintain antispyware software_**–Spyware is software installed without your knowledge or consent that can collect your personal information and monitor your online activity. Signs that your machine could be infected by spyware include sudden multiple pop up ads, slowed performance, or being redirected to a site you did not choose to go to. Some anti-virus software also includes anti-spyware software. Keep this software updated regularly to keep the latest invasion tactics out of your machine. To avoid spyware you shouldn't click on links in emails from unknown senders and download software only from sites you know and trust. Piggybacking spyware can be unseen cost of many "free" programs.

5. **Use strong passwords** – Create passwords that are at least eight characters with upper and lower case letters and numbers. Do not use information such as birthdays, maiden names, common words, or your social security number. Do not share your password with anyone and don't use the same password for all of your accounts. Don't autosave passwords in your browser. Passwords need to be changed regularly; you should not keep the same one for years.

6. **Always be wary of attachments -** Always make sure you know the sender prior to opening an attachment received in an email or an IM. Even if the attachment is sent from a trusted source, always read through the message that accompanies it, and if anything is suspect, don't open it. Many viruses propagate by sending themselves as email attachments to the host computer's entire address book.

7. **Use flash drives cautiously -** Disable auto-run in Windows so nothing will automatically launch when you insert a new drive. Always perform a scan on flash drives prior to opening files saved on them. Never open files that you are not expecting to be on the device.

8. **Operating System and Program Patches -** Knowing when to patch products and how often patches need to be applied are some of the questions that most home users never think about. More and more programs are now offering auto update of their software allowing for applying patches every time the program needs to be updated. Although these updates don't always mean it is for the sake of security, a security patch may be issued along with the update. Microsoft Windows offers windows updates automatically. So updating windows is easier than ever when users choose this option. Knowing what else to patch other than operating system patches is important as well. Any program that acts as a server or accesses the Internet are avenues for attack. These programs need to be patched when one is available. Programs like email, browsers, flash programs, PDF programs, etc. need to be patched if one is available. If any of your programs do not have auto update capabilities, it is a good idea to check for patches to your software products at least once per month. If you use your computer on a daily basis, or the computer stays online constantly, such as with high speed connections, you may need to consider a more aggressive schedule for patches.